Fig. 1

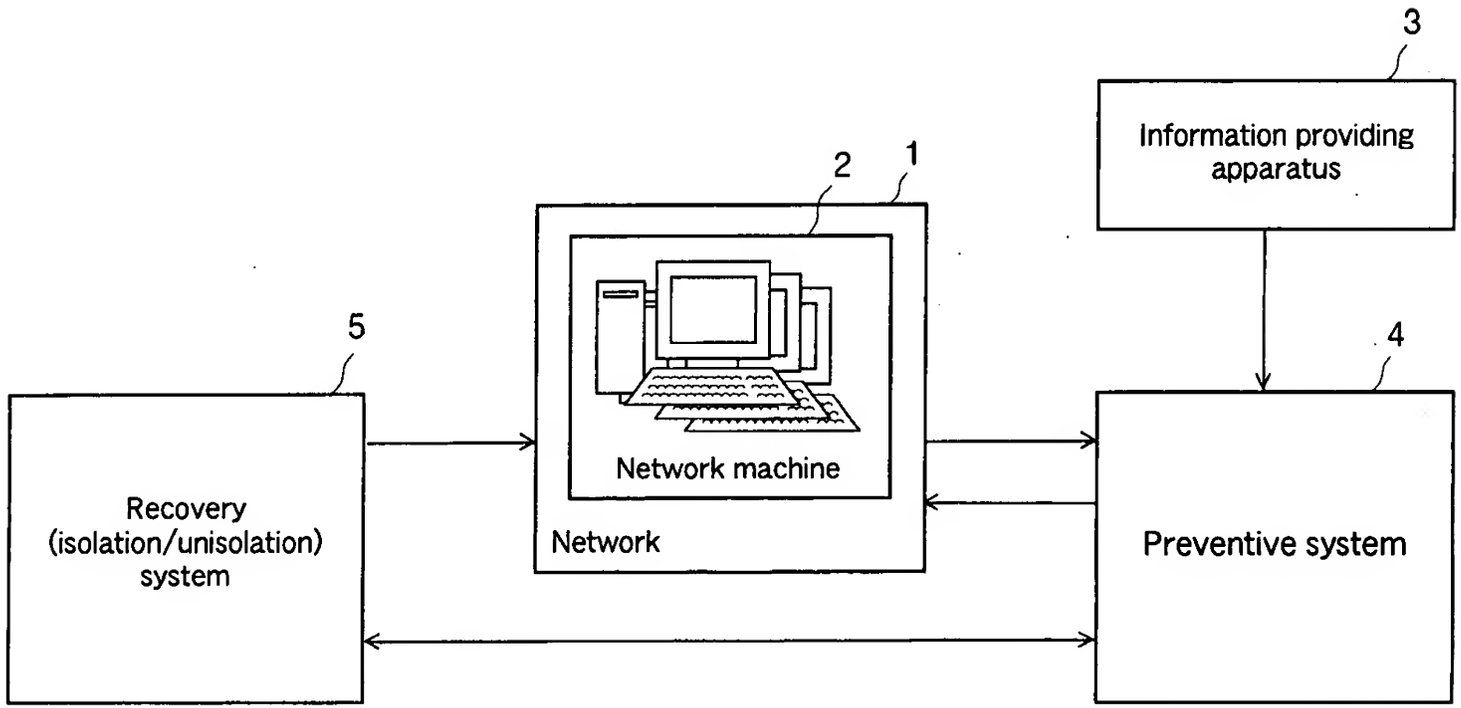

3
Information providing apparatus
2
1
5
4
Network machine
Network
Recovery (isolation/unisolation) system
Preventive system

Fig. 2

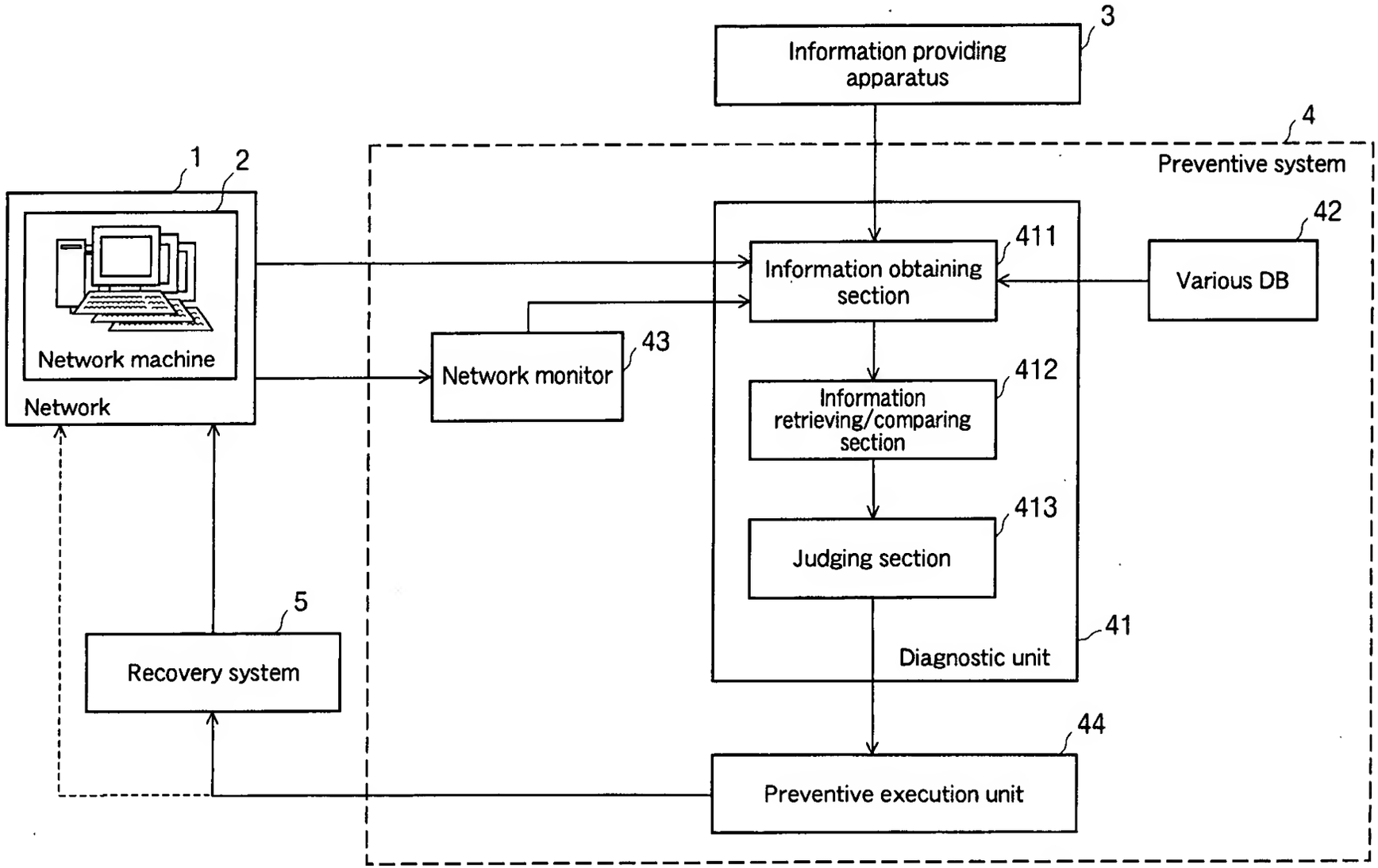

Information providing apparatus
3
4
Preventive system
1
2
Network machine
Network
Network monitor
43
411
Information obtaining section
42
Various DB
412
Information retrieving/comparing section
413
Judging section
41
Diagnostic unit
5
Recovery system
44
Preventive execution unit

Fig. 3

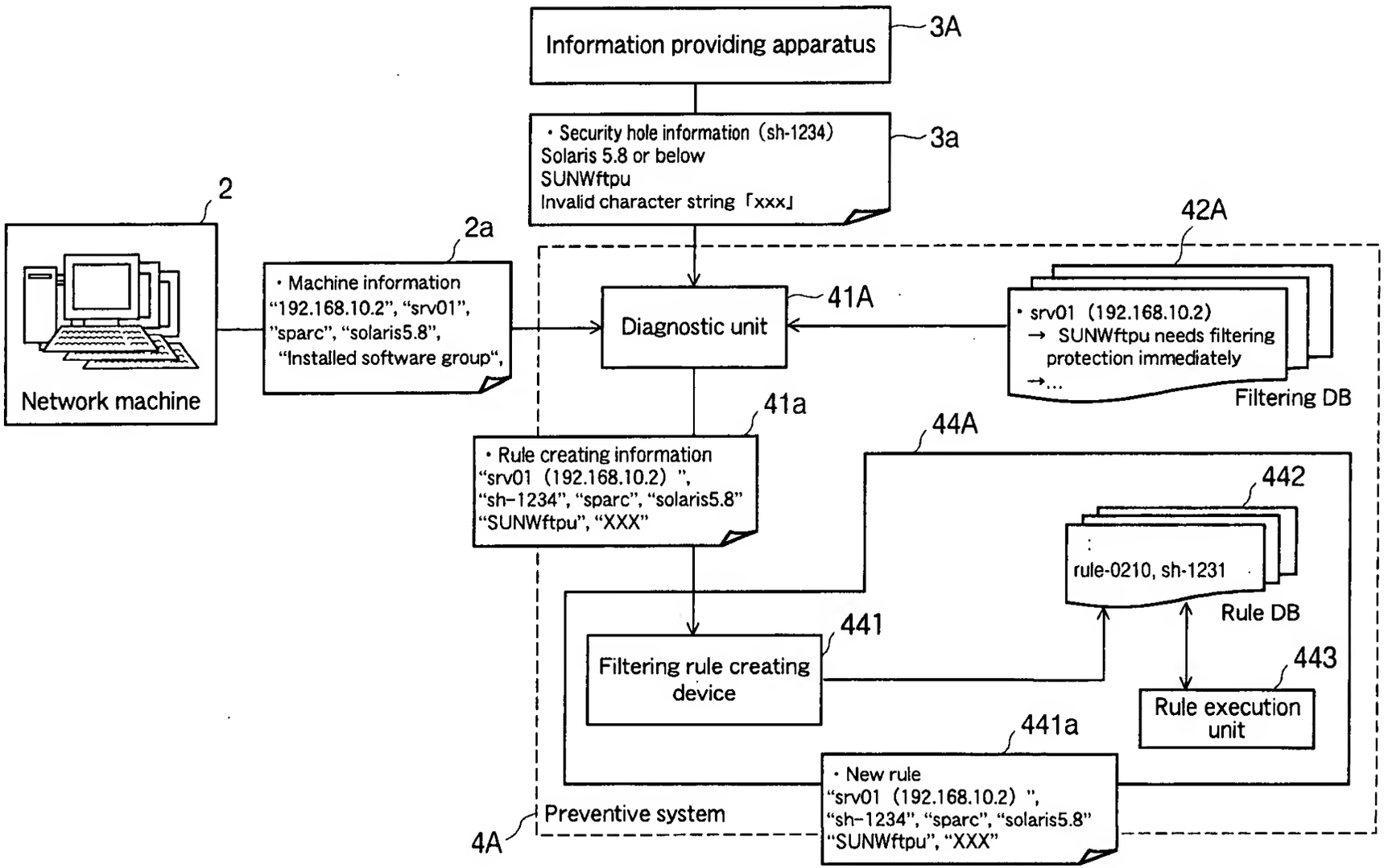

Information providing apparatus
3A
・Security hole information (sh-1234)
Solaris 5.8 or below
SUNWftpu
Invalid character string「xxx」
3a
2
2a
・Machine information
"192.168.10.2", "srv01",
"sparc", "solaris5.8",
"Installed software group",
Network machine
Diagnostic unit
41A
42A
・srv01 (192.168.10.2)
→ SUNWftpu needs filtering
protection immediately
→...
Filtering DB
41a
・Rule creating information
"srv01 (192.168.10.2) ",
"sh-1234", "sparc", "solaris5.8"
"SUNWftpu", "XXX"
44A
442
rule-0210, sh-1231
Rule DB
441
Filtering rule creating device
443
Rule execution unit
441a
・New rule
"srv01 (192.168.10.2) ",
"sh-1234", "sparc", "solaris5.8"
"SUNWftpu", "XXX"
Preventive system
4A

Fig. 4

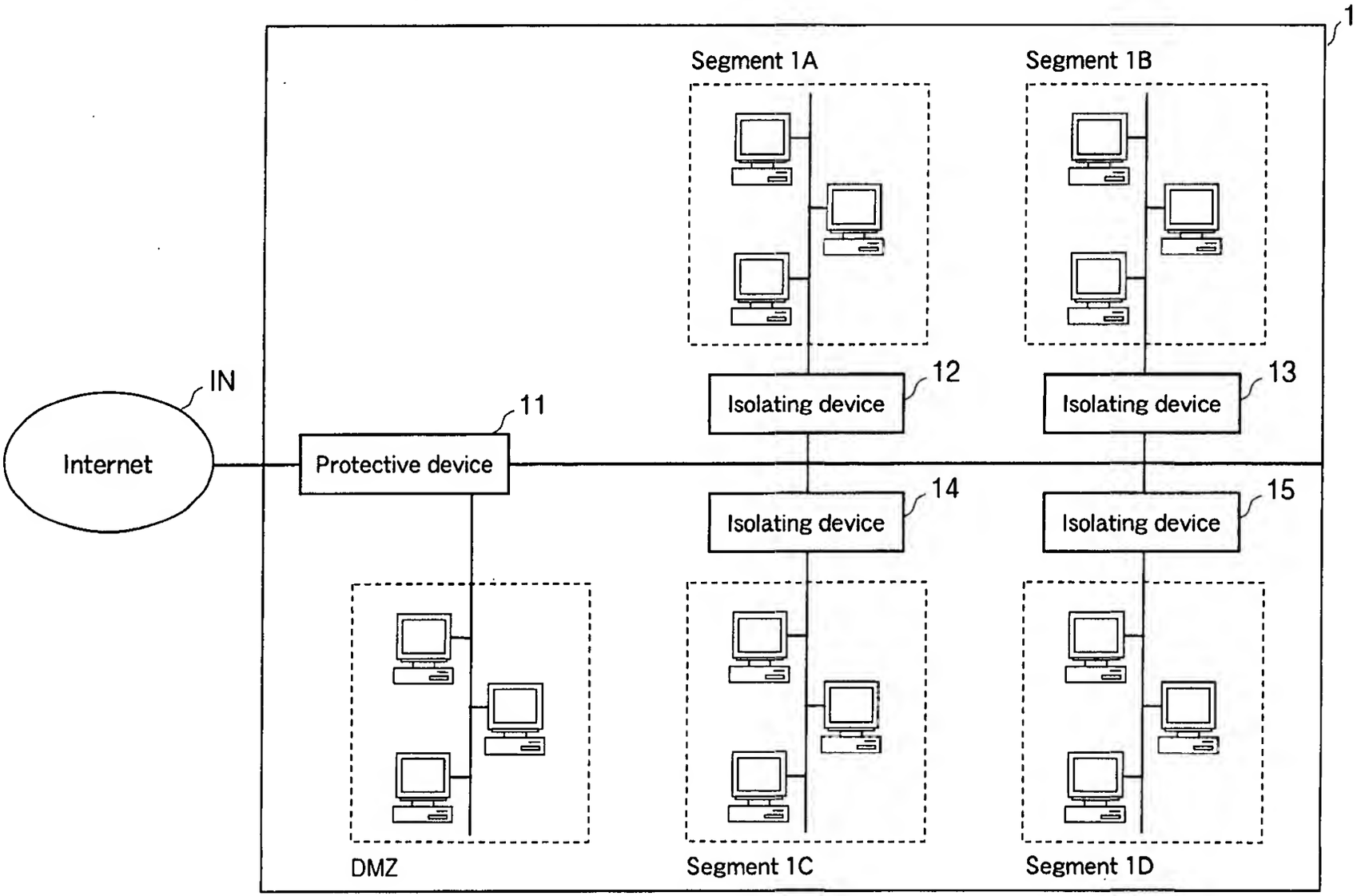

1
Segment 1A
Segment 1B
IN
Internet
11
Protective device
12
Isolating device
13
Isolating device
14
Isolating device
15
Isolating device
DMZ
Segment 1C
Segment 1D

Fig. 5

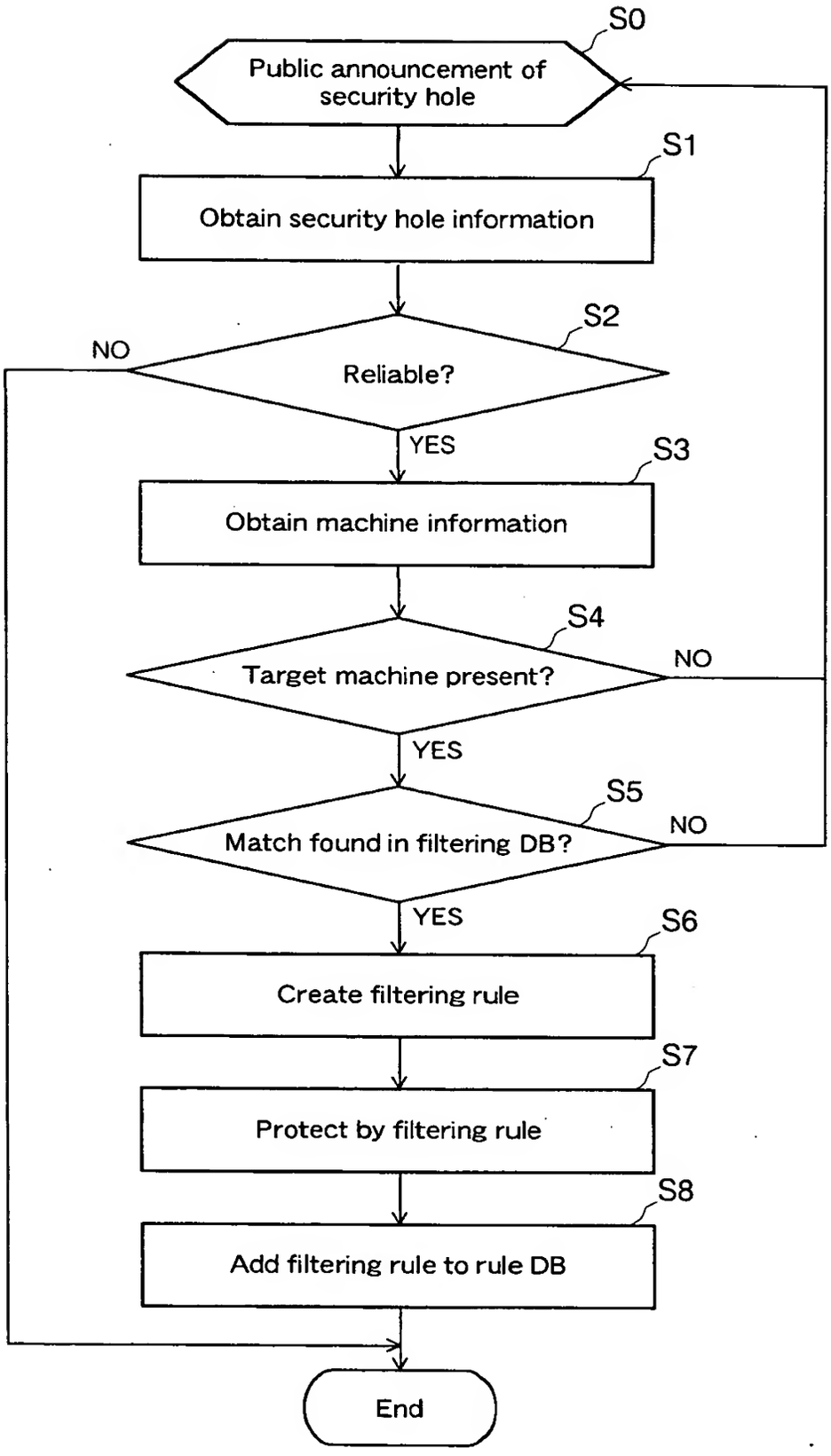

S0
Public announcement of security hole
S1
Obtain security hole information
S2
Reliable?
NO
YES
S3
Obtain machine information
S4
Target machine present?
NO
YES
S5
Match found in filtering DB?
NO
YES
S6
Create filtering rule
S7
Protect by filtering rule
S8
Add filtering rule to rule DB
End

Fig. 6

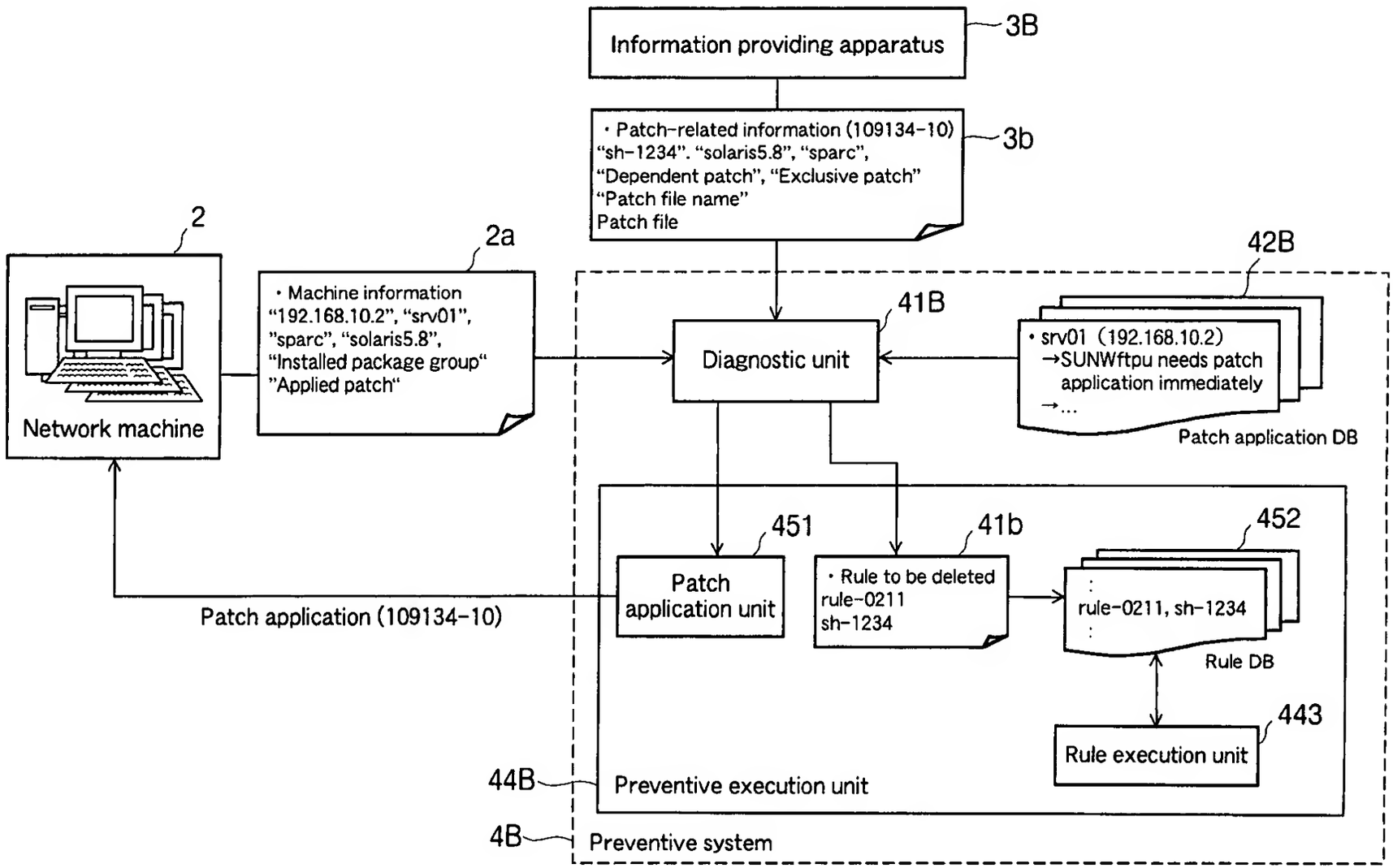

Information providing apparatus
3B
・Patch-related information (109134-10)
"sh-1234", "solaris5.8", "sparc",
"Dependent patch", "Exclusive patch"
"Patch file name"
Patch file
3b
2
2a
42B
41B
・Machine information
"192.168.10.2", "srv01",
"sparc", "solaris5.8",
"Installed package group"
"Applied patch"
Diagnostic unit
・srv01 (192.168.10.2)
→SUNWftpu needs patch
application immediately
→...
Patch application DB
Network machine
451
41b
452
Patch
application unit
・Rule to be deleted
rule-0211
sh-1234
rule-0211, sh-1234
Rule DB
Patch application (109134-10)
443
Rule execution unit
44B
Preventive execution unit
4B
Preventive system

Fig. 7

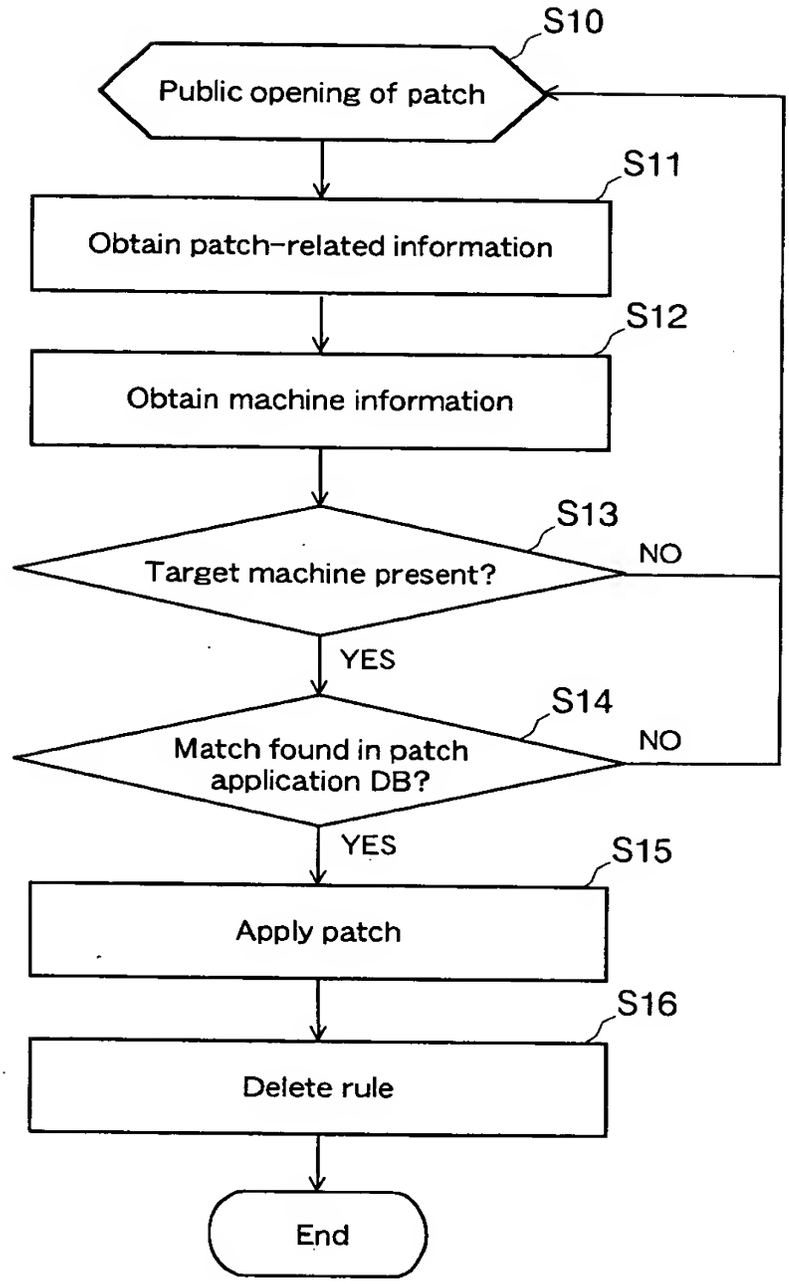

S10
Public opening of patch
S11
Obtain patch-related information
S12
Obtain machine information
S13
Target machine present?
NO
YES
S14
Match found in patch application DB?
NO
YES
S15
Apply patch
S16
Delete rule
End

Fig. 8

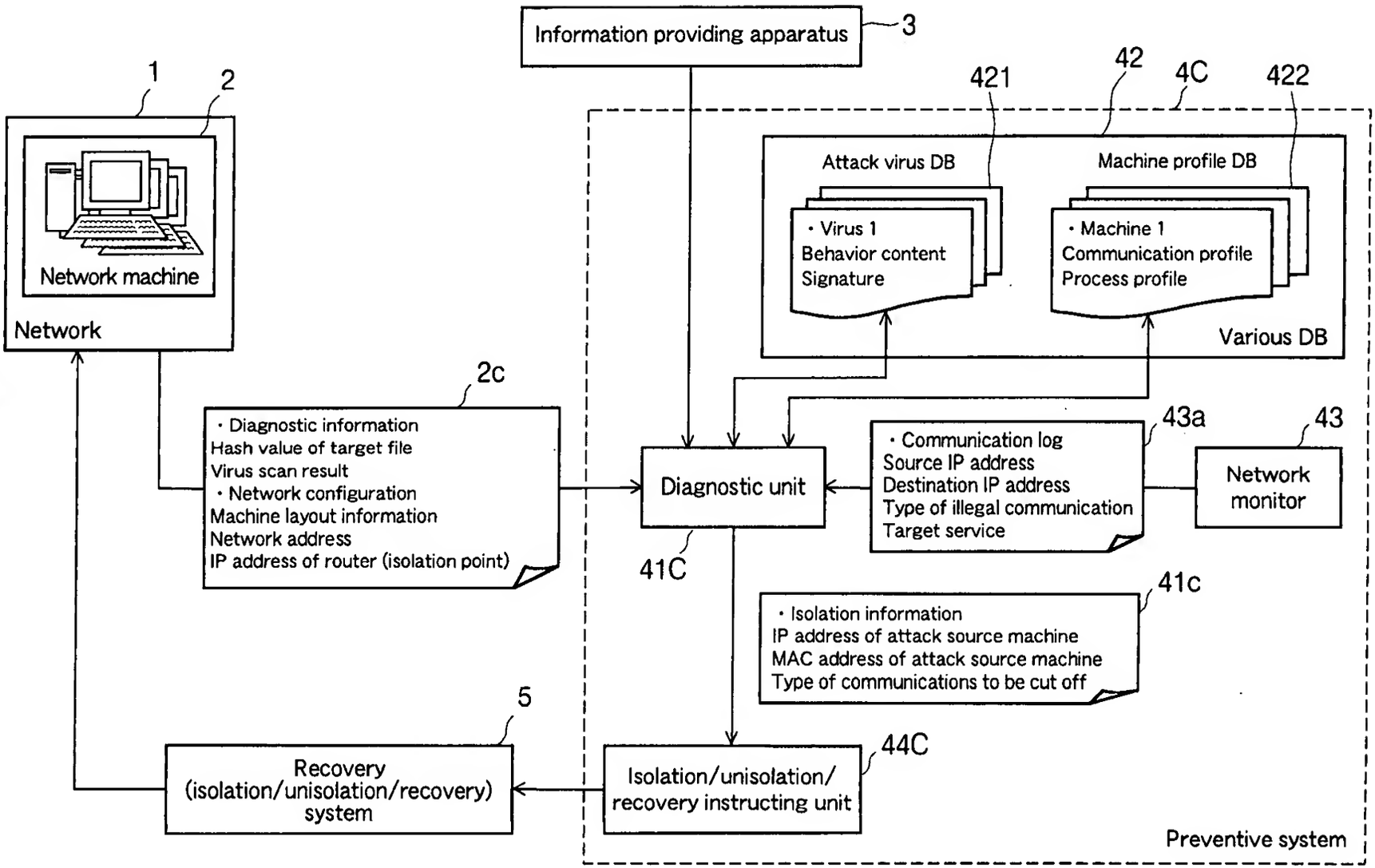

Information providing apparatus
3
1
2
Network machine
Network
421
42
4C
422
Attack virus DB
Machine profile DB
・Virus 1
Behavior content
Signature
・Machine 1
Communication profile
Process profile
Various DB
2c
・Diagnostic information
Hash value of target file
Virus scan result
・Network configuration
Machine layout information
Network address
IP address of router (isolation point)
Diagnostic unit
41C
43a
・Communication log
Source IP address
Destination IP address
Type of illegal communication
Target service
43
Network monitor
41c
・Isolation information
IP address of attack source machine
MAC address of attack source machine
Type of communications to be cut off
5
Recovery (isolation/unisolation/recovery) system
Isolation/unisolation/ recovery instructing unit
44C
Preventive system

Fig. 9

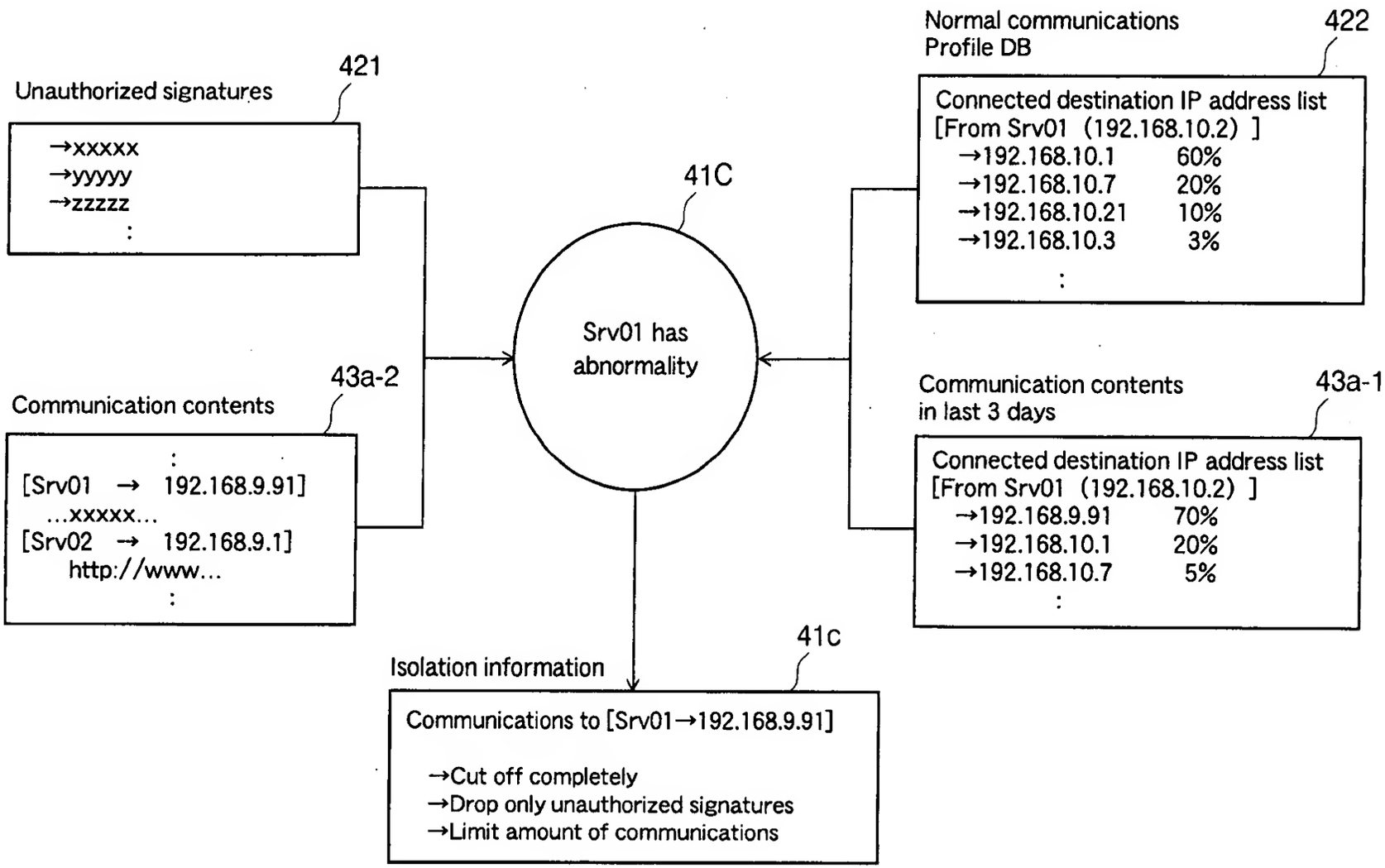

Normal communications
Profile DB
422
Unauthorized signatures
421
→xxxxx
→yyyyy
→zzzzz
:
Connected destination IP address list
[From Srv01 (192.168.10.2)]
→192.168.10.1 60%
→192.168.10.7 20%
→192.168.10.21 10%
→192.168.10.3 3%
:
41C
Srv01 has
abnormality
43a-2
Communication contents
:
[Srv01 → 192.168.9.91]
...xxxxx...
[Srv02 → 192.168.9.1]
http://www...
:
Communication contents
in last 3 days
43a-1
Connected destination IP address list
[From Srv01 (192.168.10.2)]
→192.168.9.91 70%
→192.168.10.1 20%
→192.168.10.7 5%
:
41c
Isolation information
Communications to [Srv01→192.168.9.91]
→Cut off completely
→Drop only unauthorized signatures
→Limit amount of communications

Fig.10

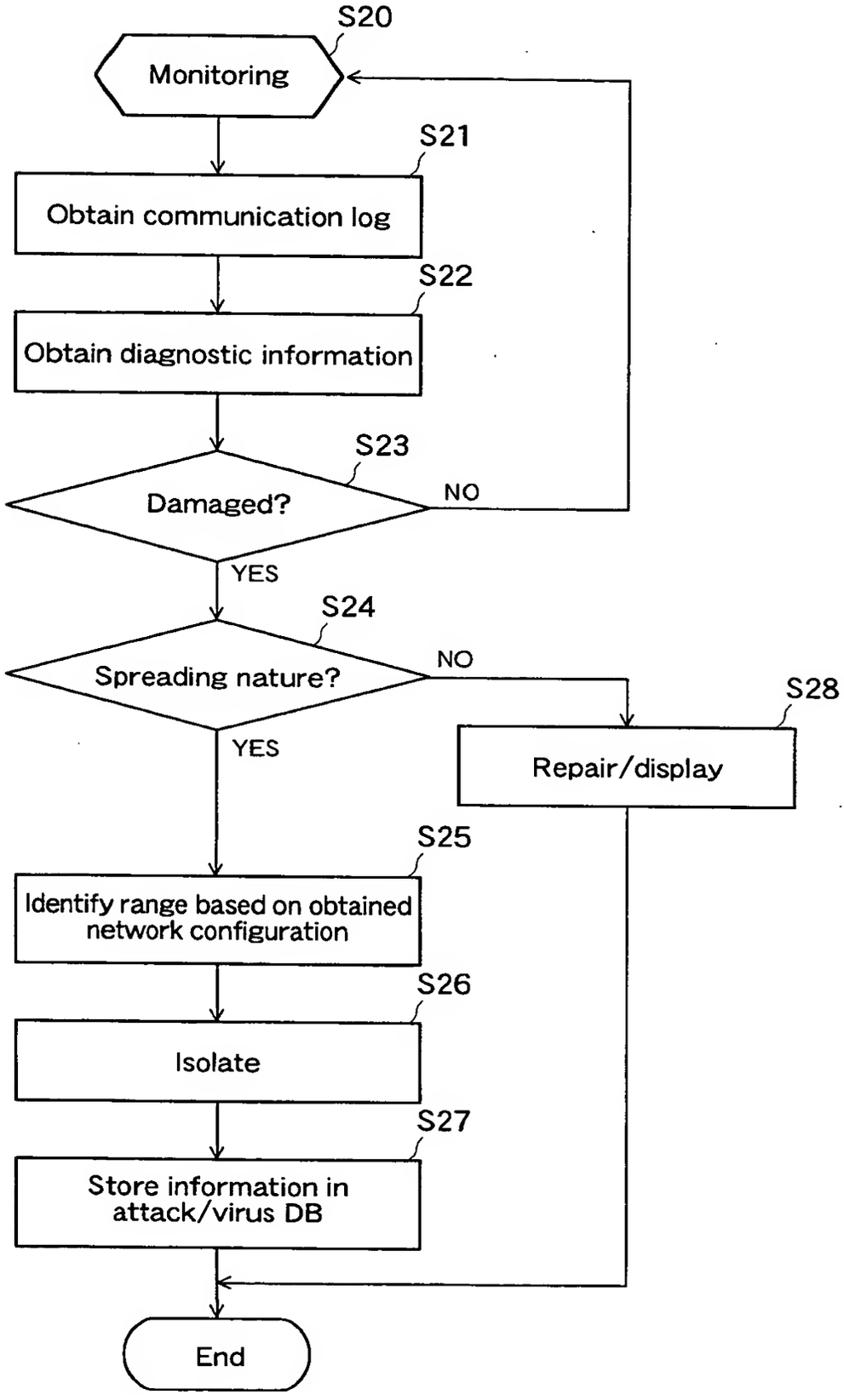

S20
Monitoring
S21
Obtain communication log
S22
Obtain diagnostic information
S23
Damaged?
NO
YES
S24
Spreading nature?
NO
YES
S28
Repair/display
S25
Identify range based on obtained network configuration
S26
Isolate
S27
Store information in attack/virus DB
End

Fig.11

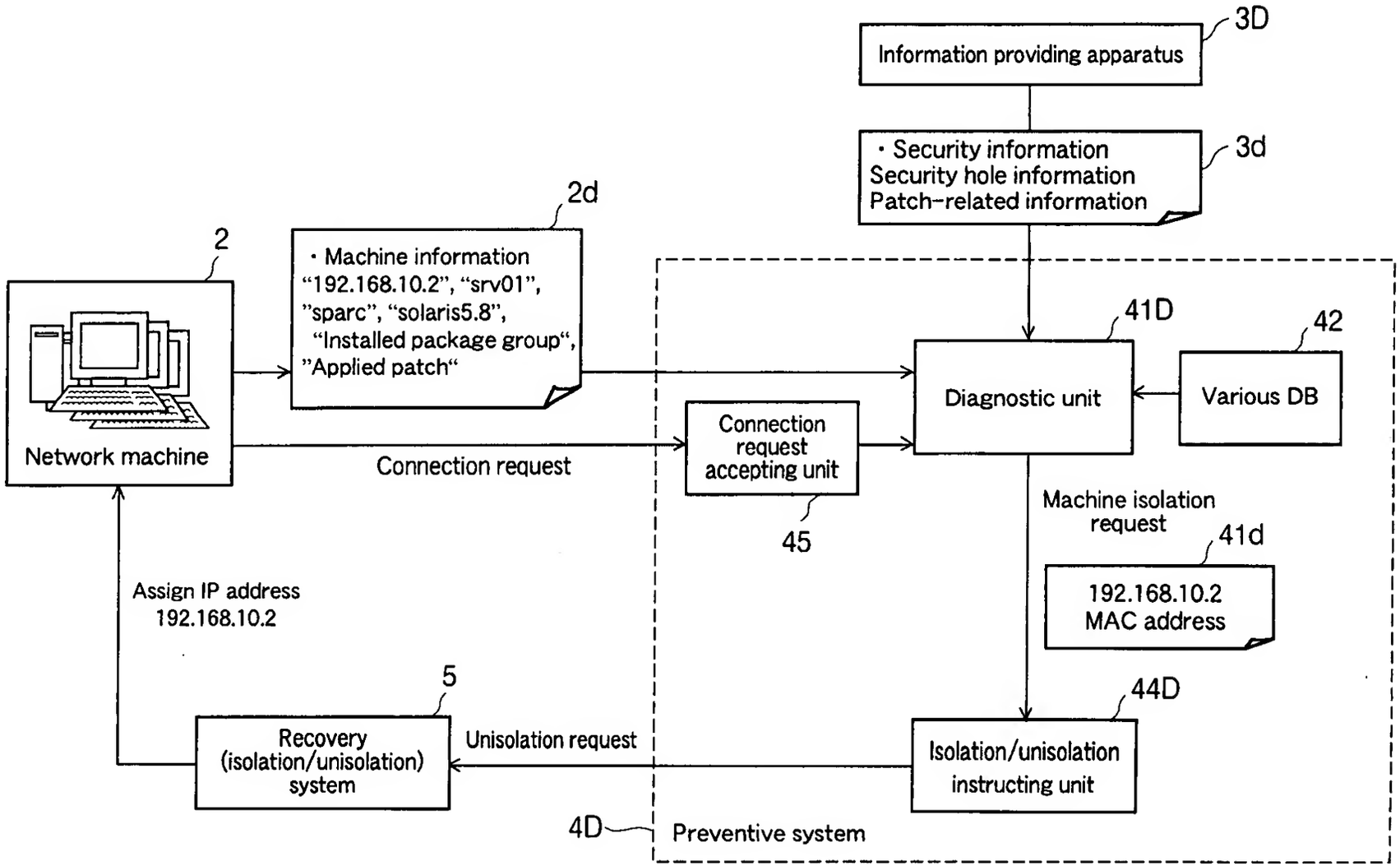

Information providing apparatus
3D
・Security information
Security hole information
Patch-related information
3d
2d
2
・Machine information
"192.168.10.2", "srv01",
"sparc", "solaris5.8",
"Installed package group",
"Applied patch"
41D
42
Diagnostic unit
Various DB
Network machine
Connection request
Connection request accepting unit
45
Machine isolation request
41d
192.168.10.2
MAC address
Assign IP address
192.168.10.2
5
44D
Recovery (isolation/unisolation) system
Unisolation request
Isolation/unisolation instructing unit
4D
Preventive system

Fig.12

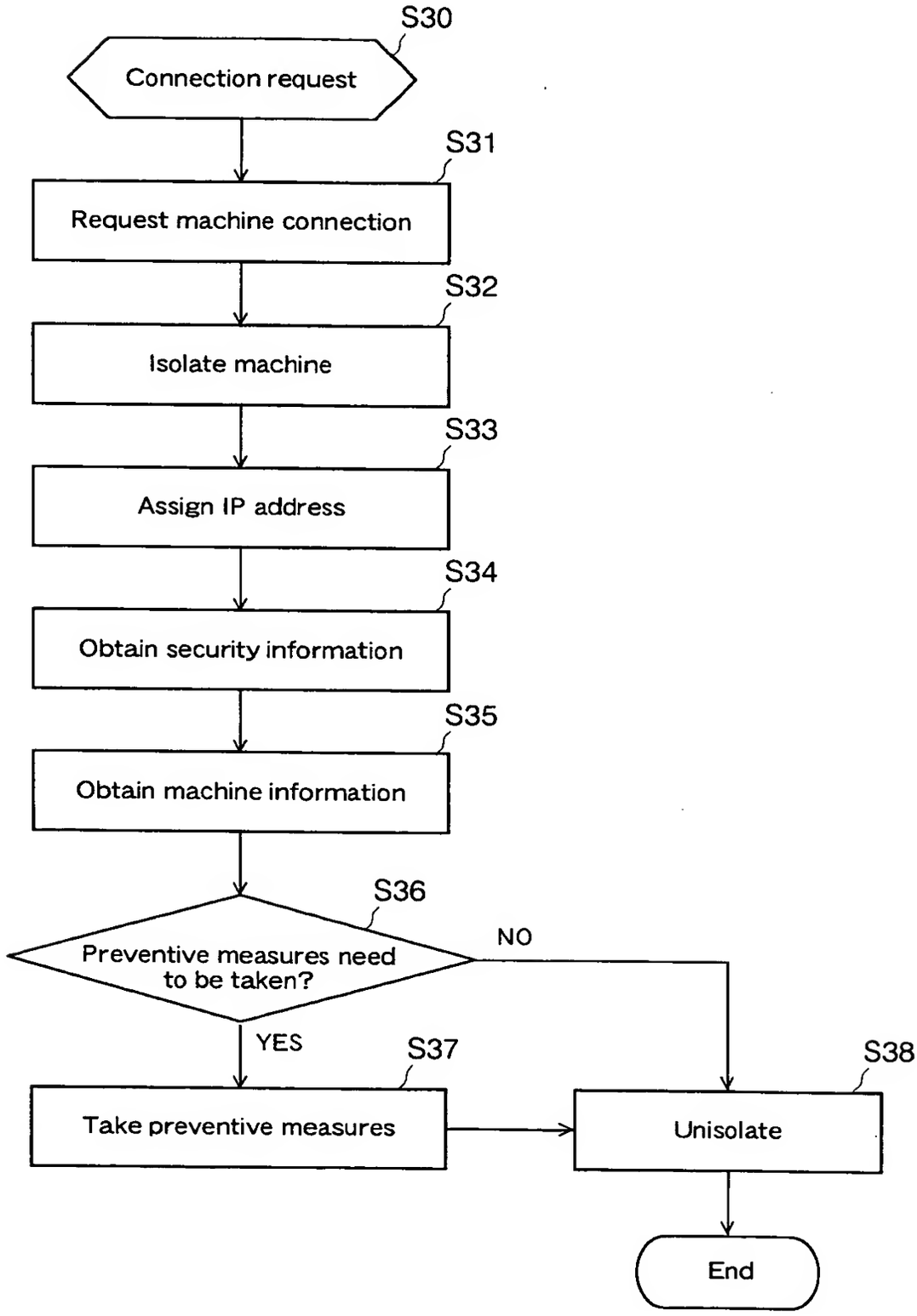

S30
Connection request
S31
Request machine connection
S32
Isolate machine
S33
Assign IP address
S34
Obtain security information
S35
Obtain machine information
S36
Preventive measures need to be taken?
NO
YES
S37
Take preventive measures
S38
Unisolate
End

Fig.13

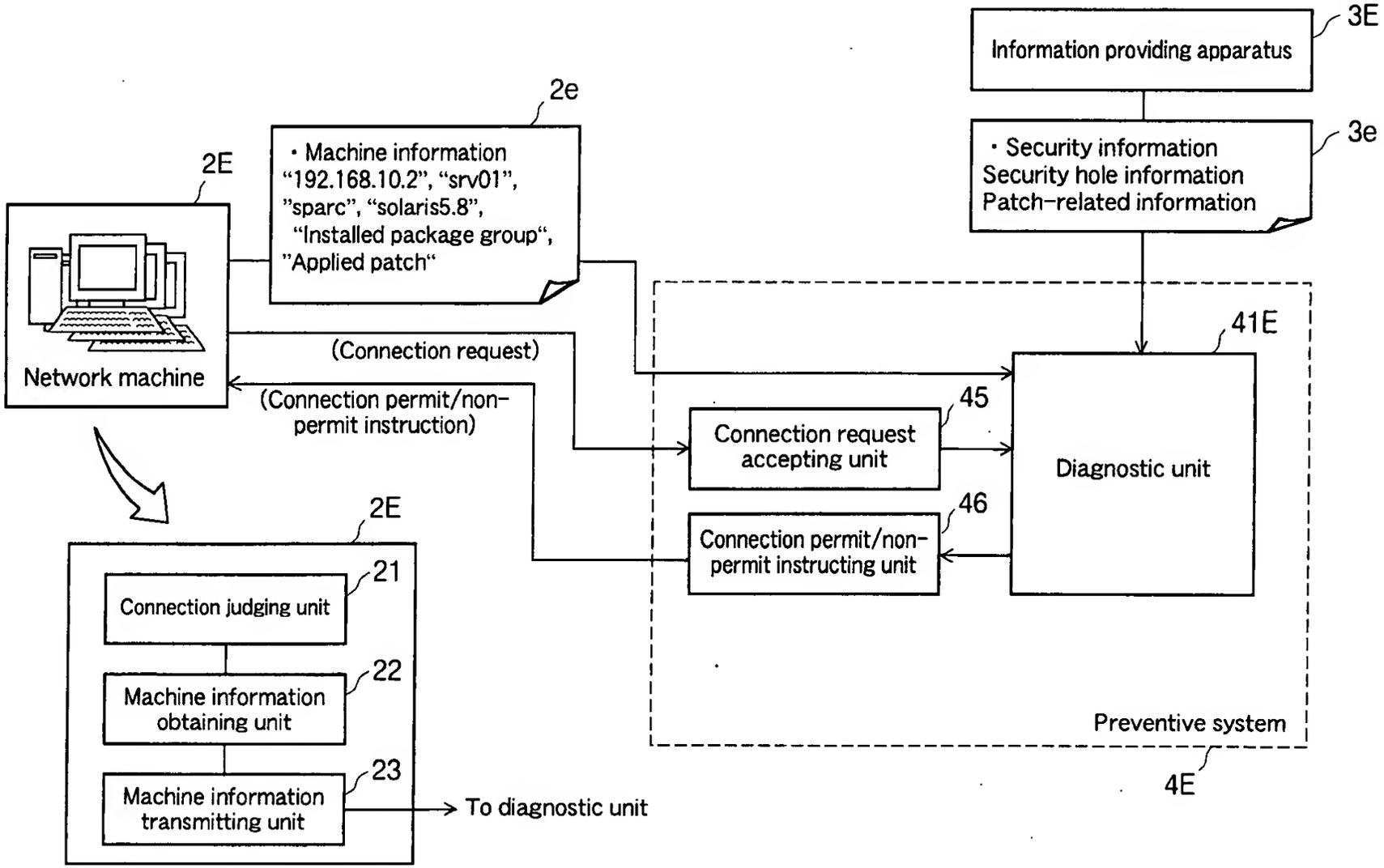

Information providing apparatus
3E
2e
・Machine information
"192.168.10.2", "srv01",
"sparc", "solaris5.8",
"Installed package group",
"Applied patch"
3e
・Security information
Security hole information
Patch-related information
2E
Network machine
(Connection request)
(Connection permit/non-permit instruction)
41E
45
Connection request accepting unit
Diagnostic unit
46
Connection permit/non-permit instructing unit
2E
21
Connection judging unit
22
Machine information obtaining unit
23
Machine information transmitting unit
To diagnostic unit
Preventive system
4E

Fig.14

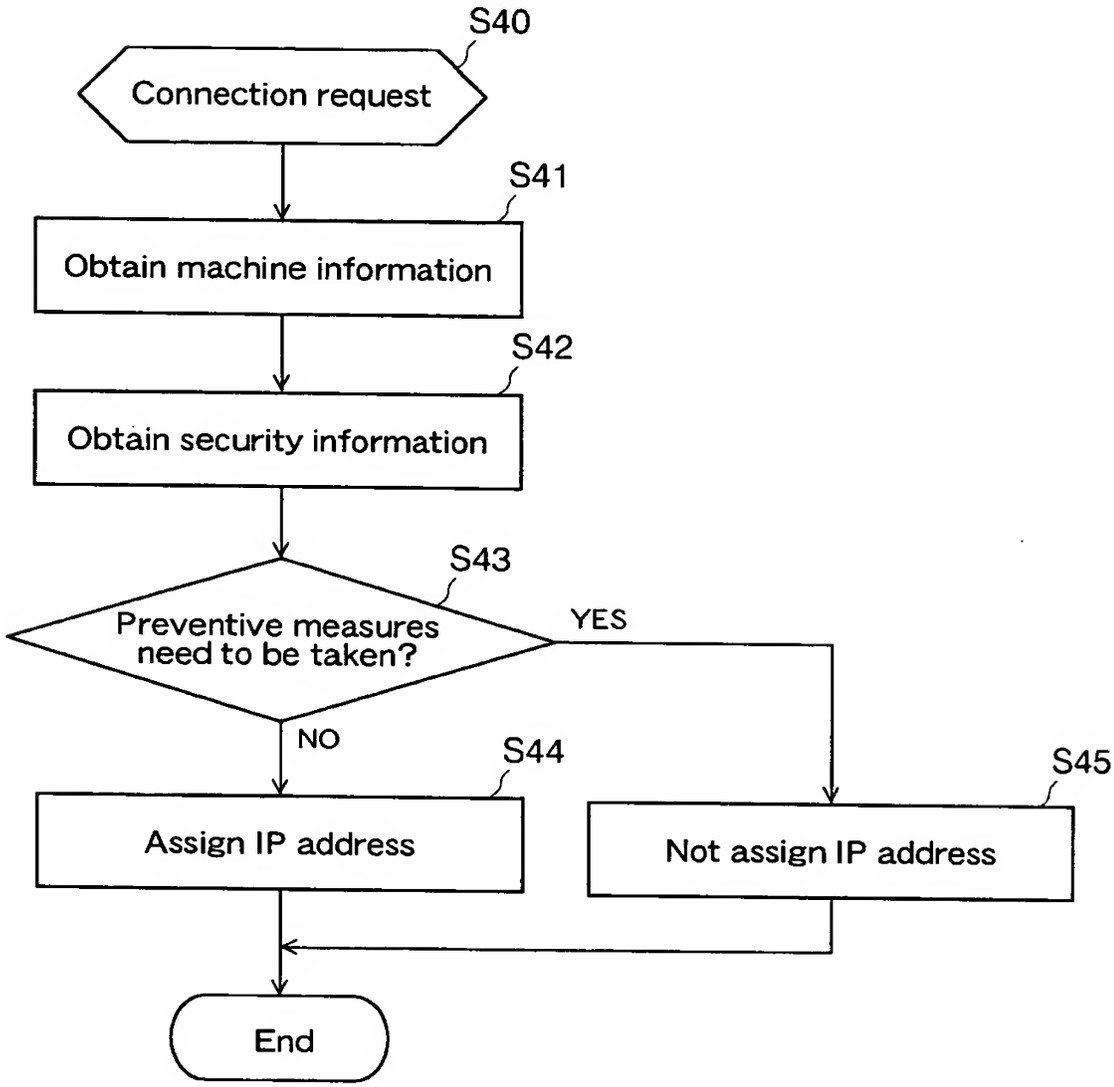

S40
Connection request
S41
Obtain machine information
S42
Obtain security information
S43
Preventive measures need to be taken?
YES
NO
S44
Assign IP address
S45
Not assign IP address
End

Fig.15

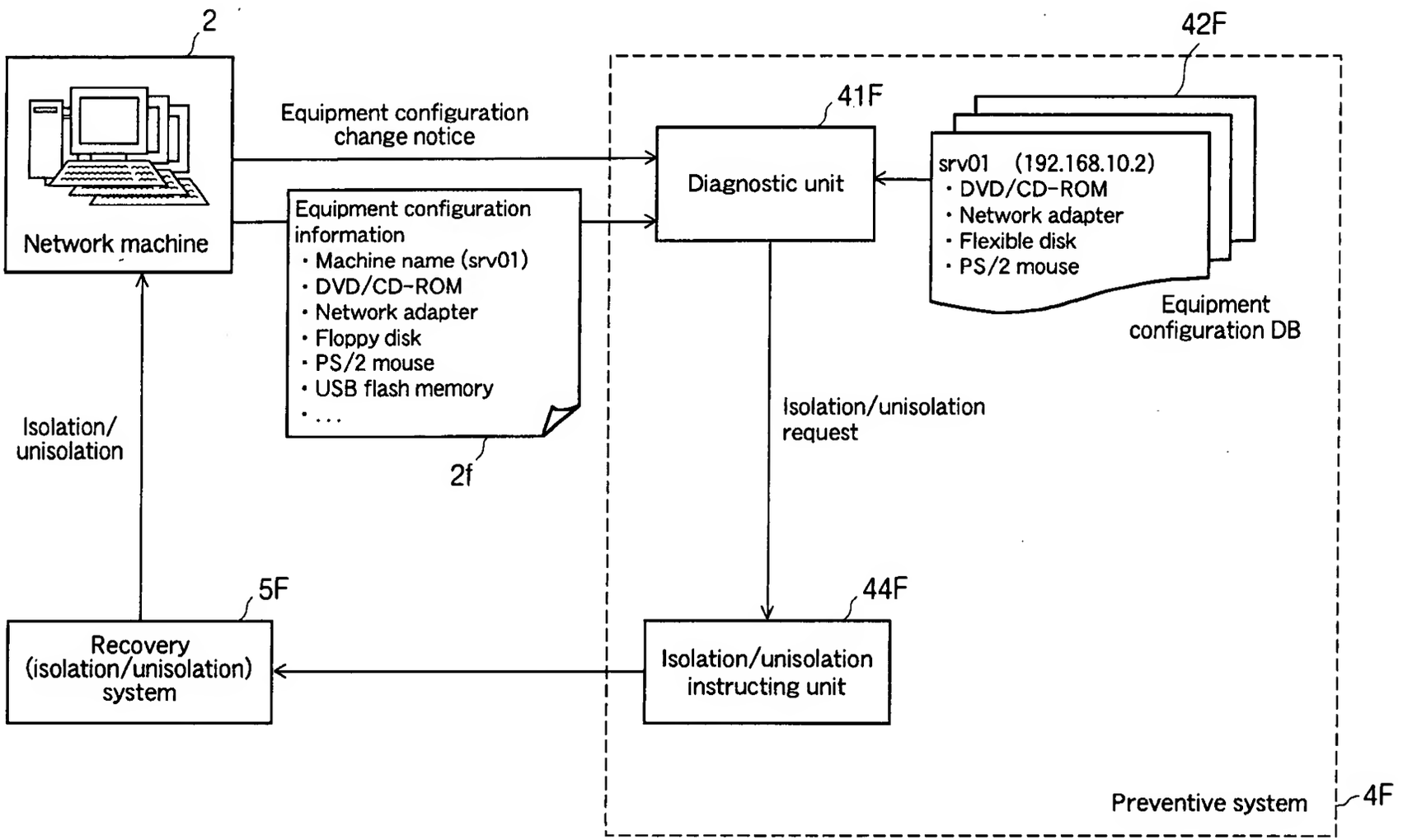

2
Network machine
Equipment configuration change notice
Equipment configuration information
• Machine name (srv01)
• DVD/CD-ROM
• Network adapter
• Floppy disk
• PS/2 mouse
• USB flash memory
• ...
2f
Isolation/ unisolation
5F
Recovery (isolation/unisolation) system
42F
41F
Diagnostic unit
srv01 (192.168.10.2)
• DVD/CD-ROM
• Network adapter
• Flexible disk
• PS/2 mouse
Equipment configuration DB
Isolation/unisolation request
44F
Isolation/unisolation instructing unit
Preventive system
4F

Fig.16

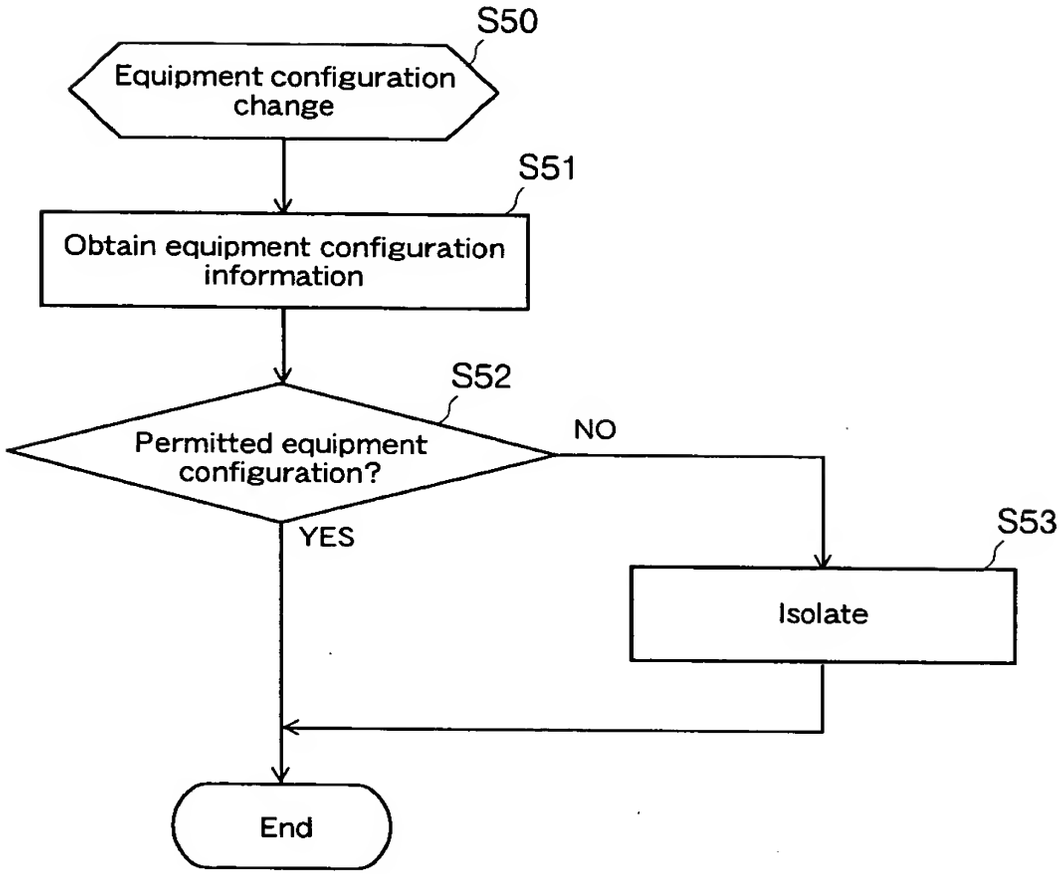

S50
Equipment configuration change
S51
Obtain equipment configuration information
S52
Permitted equipment configuration?
NO
YES
S53
Isolate
End

Fig.17

```
[SERVER_NAME]
srv01
[ARCHITECTURE]
sparc
[OS_VERSION]
5.8
[HARDWARE]
SUNW,SPARCstation-20
[INSTALL_PACKAGE]
SUNWadmap
SUNWftpr
SUNWftpu
:
[APPLY_PATCH]
109134-10
109134-27
109618-01
:
[END]
```

Fig.18

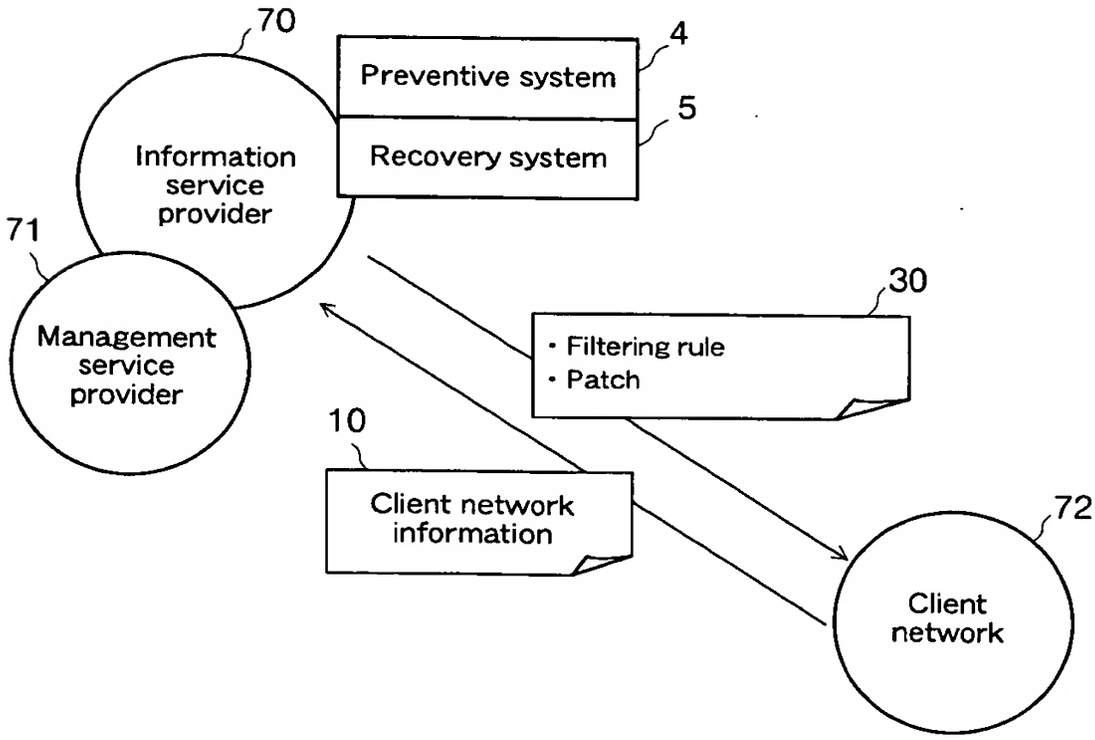


Fig.19

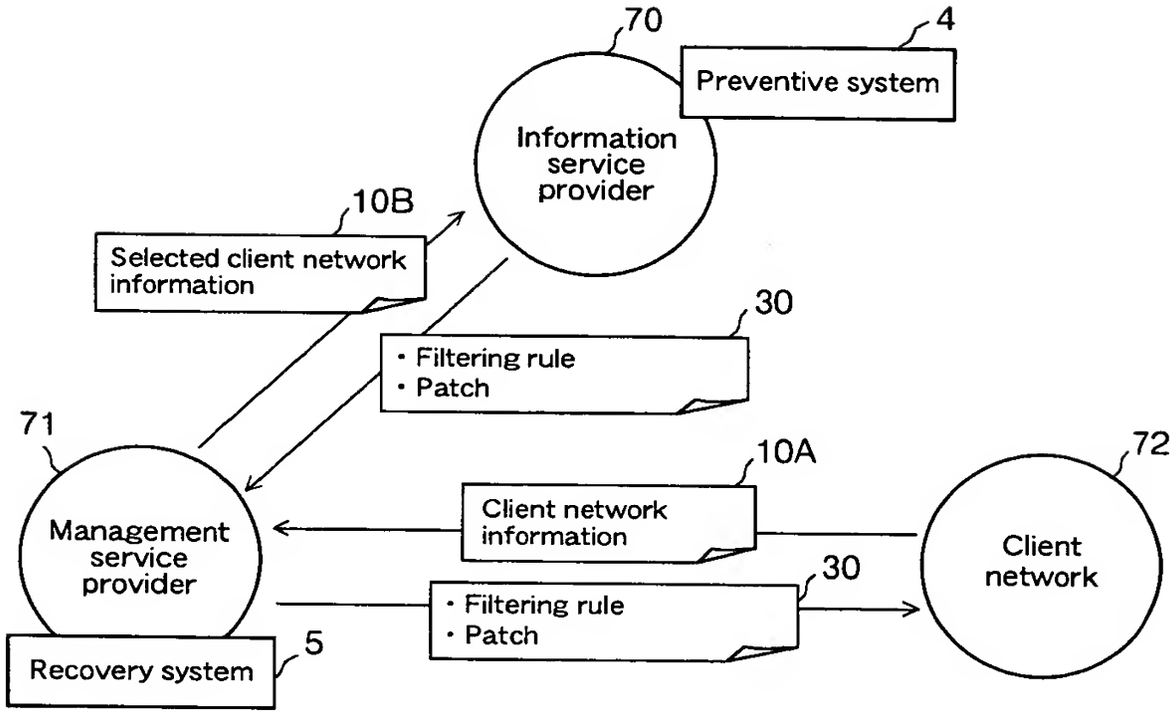

70
4
Preventive system
Information service provider
10B
Selected client network information
30
• Filtering rule
• Patch
71
10A
72
Management service provider
Client network information
Client network
30
• Filtering rule
• Patch
Recovery system
5

Fig.20

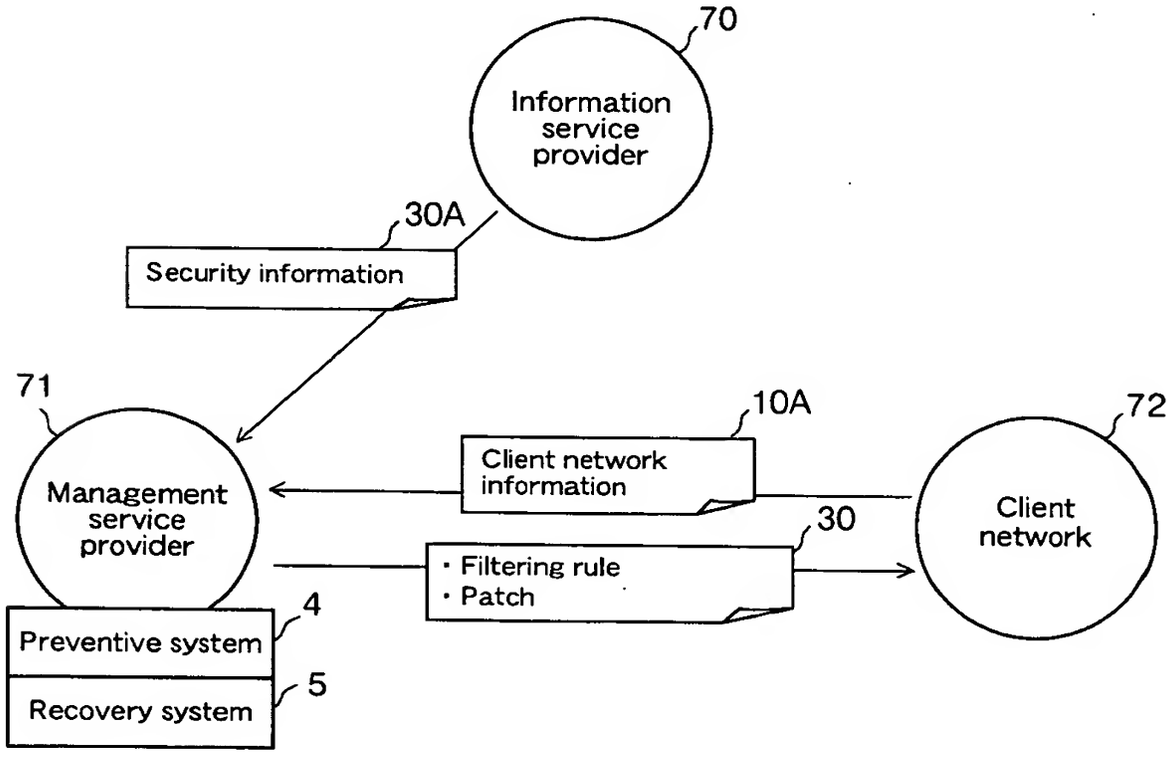
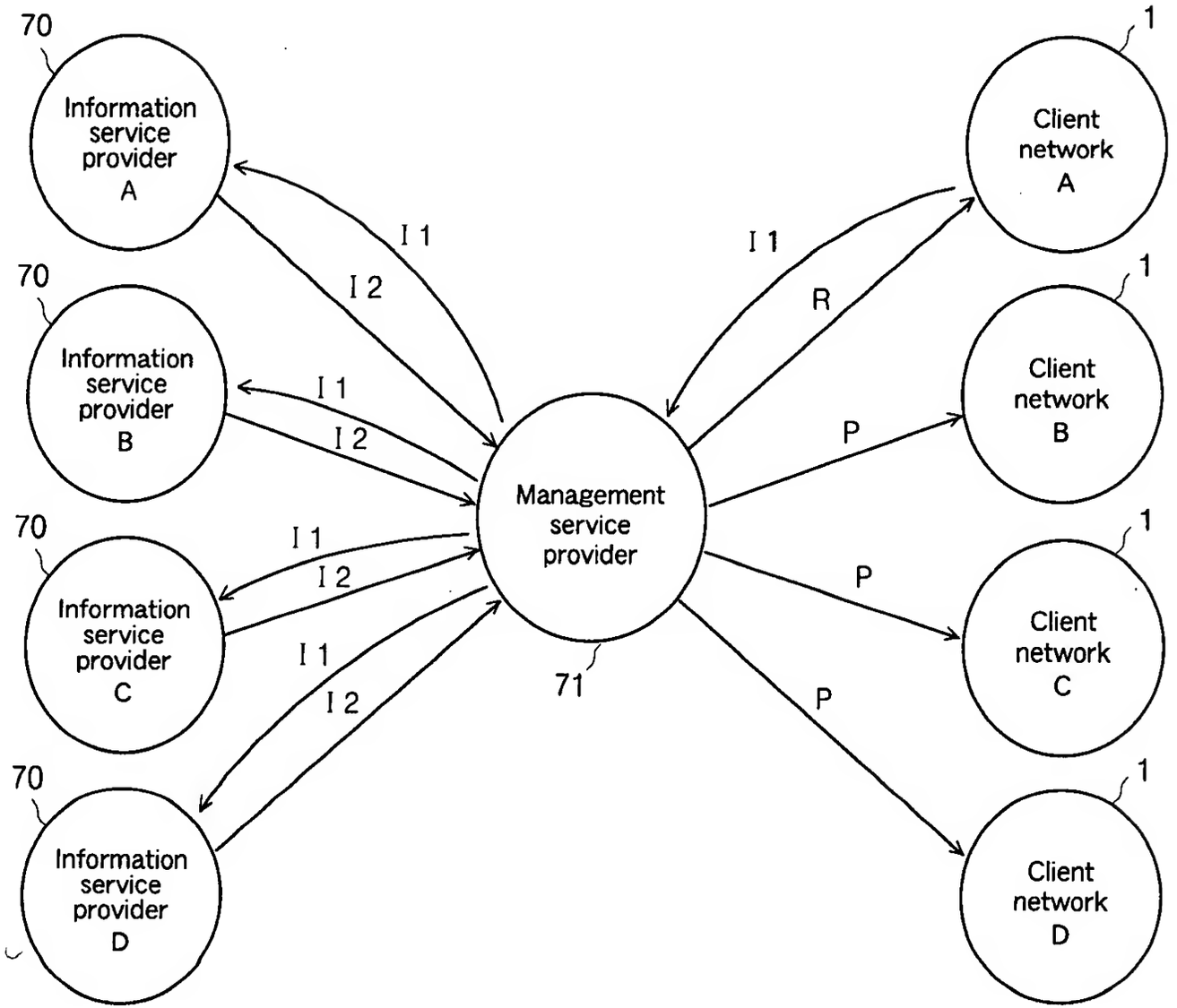

70
Information service provider
30A
Security information
71
10A
72
Management service provider
Client network information
Client network
30
• Filtering rule
• Patch
4
Preventive system
5
Recovery system

Fig.21


70
Information service provider A
70
Information service provider B
70
Information service provider C
70
Information service provider D
I 1
I 2
I 1
I 2
I 1
I 2
I 1
I 2
Management service provider
71
I 1
R
P
P
P
1
Client network A
1
Client network B
1
Client network C
1
Client network D